Listing of Claims:

1. (Currently amended) A method for use in managing resources ~~for IP~~ in networking, the method comprising:

adding a field to an operating system kernel software procedure, the field referencing a virtual router context; and

modifying packet processing software code to cause the packet processing software code to execute in accordance with the virtual router context.

2. (New) A method for using a network device having an operating system instance that operates in a plurality of routing contexts, the method comprising:

associating a first network with a first routing context and a second network with a second routing context, wherein the first context is isolated from the second context;

receiving, at the same networking address, a first message originating from the first network and a second message originating from the second network by the network device;

associating the first message with a first application running on the operating system instance of the network device based on a determination that the first message is associated with the first routing context; and

associating the second message with a second application running on the operating system instance based on a determination that the second message is associated with the second routing context.

3. (New) The method of claim 2, wherein at least one of Transport Control Protocol (TCP), User Datagram Protocol (UDP), and raw IP code associated with the operating system instance is modified to cause the code to execute in accordance with a particular routing context.

4. (New) The method of claim 2, further comprising:

assigning to the first message a first routing context number, wherein the first message is determined to be associated with the first routing context using the first routing context number; and

assigning to the second message a second routing context number, wherein the second

message is determined to be associated with the second routing context using the second routing context number.

5. (New) The method of claim 4, further comprising:

assigning a first routing table to the first router context, wherein the first routing table is associated with the first context number; and

assigning a second routing table to the second router context, wherein the second routing table is associated with the second context number.

6. (New) The method of claim 2, wherein the first and second networks are private networks that are isolated from the Internet.

7. (New) The method of claim 2, wherein information received by the network device from the first network is not provided to the second network by the network device, and wherein information received by the network device from the second network is not provided to the first network by the network device.

8. (New) The method of claim 2, wherein both the first message and the second message include at least one data packet.

9. (New) The method of claim 2, wherein the first and second messages are received by the network device using a first network connection initiated by a first process and a second network connection initiated by a second process, respectively, the method further comprising:

assigning to the first process a default first routing context number; and

assigning to the second process a default second routing context number.

10. (New) The method of claim 9, further comprising inheriting the default first routing context by a third process, whose parent is the first process, at the time of creation of the third process.

11. (New) The method of claim 2, further comprising associating at least one interface to the operating system instance with a routing context.

12. (New) A computer system comprising:

a first network that is associated with a first routing context;

a second network that is associated with a second routing context;

a network device that receives messages from both the first network and second network at a single networking address, wherein the network device is configured to determine that messages received from the first network are associated with the first routing context and to determine that messages received from the second network are associated with the second routing context.

13. (New) A method for using a plurality of processors running on different operating system instances to implement a distributed IP host, the method comprising:

receiving an ingress packet to be processed;

determining, when possible, which of the plurality of processors will be the consumer of the ingress packet;

sending the ingress packet, when one of the plurality of processors is determined to be the consumer of the ingress packet, to the one of the plurality of processors;

sending the ingress packet, when it is not determined which of the plurality of processors will be the consumer of the ingress packet, to each of the plurality of processors;

designating one of the plurality of processors as the lead processor of the distributed IP host, wherein the lead processor processes ingress packets that do not correspond to any specific port of the IP host.

14. (New) The method of claim 13, wherein a network processor subsystem is used to determine which of the plurality of processors will be the consumer of the ingress packet.

15. (New) The method of claim 13, wherein a Media Access Control broadcast is used when sending the ingress packet to each of the plurality of processors.

16. (New) The method of claim 13, further comprising adding an extension that is used for designating whether a particular interface of the distributed IP host is the lead interface for the distributed IP host.

17. (New) The method of claim 16, wherein the extension is one of a procfs extension and a netlink extension.

18. (New) The method of claim 16, further comprising modifying Address Resolution Protocol (ARP) code such that non-lead interfaces of the distributed IP host do not respond to ARP requests.

19. (New) The method of claim 13, wherein at least one of Transport Control Protocol (TCP) and User Datagram Protocol (UDP) code is modified such that the ingress packet is ignored when it arrives at a port that is not locally bound.

20. (New) The method of claim 13, further comprising modifying Internet Control Messaging Protocol (ICMP) code such that, when the ingress packet is an ICMP packet that is correlated with a specific port, the ICMP packet is ignored by the distributed IP host unless the specific port is bound.